In The United States Patent and Trademark Office
On Appeal From The Examiner To The Board
of Patent Appeals and Interferences

In re Application of:	Dennis Cox et al.
Serial No.:	10/808,629
Filing Date:	March 24, 2004
Group Art Unit:	2136
Examiner:	Chinwendu C. Okoronkwo
Confirmation No.:	6090
Title:	Method for Blocking Denial of Service and Address Spoofing Attacks on a Private Network

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Appeal Brief

Appellants have appealed to the Board of Patent Appeals and Interferences ("Board") from the decision of the Examiner mailed March 4, 2008, finally rejecting pending Claims 1-33 ("Final Office Action"). Appellants received an Advisory Action on May 29, 2008 ("Advisory Action") maintaining the rejections of the Final Office Action. Appellants filed a Notice of Appeal on July 3, 2008. Appellants respectfully submit this Appeal Brief.

Table of Contents

Page

Real Party-In-Interest

The real party-in-interest for this Application is Cisco Technology, Inc., by virtue of a chain of title from the inventors to the current assignee, as shown below:

1. From: Dennis Cox
Kip McClanahan

To: Netspeed, Inc.
Assignment recorded at Reel 015226, Frame 0397,
on April 16, 2004

2. From: Netspeed, Inc.

To: Cisco Systems, Inc.
Assignment recorded at Reel 015226, Frame 0335,
on April 16, 2004

3. From: Cisco Systems, Inc.

To: Cisco Technology, Inc.
Assignment recorded at Reel 015226, Frame 0356,
on April 16, 2004

Related Appeals and Interferences

The Appellants, the undersigned Attorney for Appellants, and the Assignees know of no applications on appeal that may directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status of Claims

Claims 1-33 are pending in this Application. Claims 1-33 stand rejected pursuant to the Final Office Action mailed March 4, 2008. Specifically, Claims 1-10, 15-21, and 27-33 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,061,650 to Malkin et al. ("*Malkin*"). Claims 11-14, and 22-26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over *Malkin* in view of U.S. Application No. 2003/0053170 to Levinson et al. ("*Levinson*"). For the reasons discussed below, Appellants respectfully submit that these rejections are improper and should be reversed by the Board. Accordingly, Appellants present Claims 1-33 for Appeal and sets forth these claims in Appendix A.

Status of Amendments

All amendments submitted by Appellant were entered by the Examiner prior to the mailing of the Advisory Action on May 29, 2008.

Summary of Claimed Subject Matter

This application relates generally to communication systems, and more particularly to a method for blocking denial of service and address spoofing attacks on a private network. (pg. 1, lines 2-4).[1]

As corporate and private networks increasingly provide external access, it is important to defend the private network against outside attackers while still allowing access by authorized users. (pg. 2, lines 2-5). Routing devices may lack important safeguards to prevent attacks. (pg. 2, lines 9-10). Two forms of attack that are of particular concern are denial of service attacks and address spoofing attacks. (pg. 2, lines 11-12). Denial of service attacks may consist of sending repeated requests for connections to different hosts; if enough requests are sent to a given host, this may disrupt normal network service. (pg. 2, lines 13-18). With address spoofing, an attacker may identify a valid internal network address within a private network and then request access to the network by spoofing the valid network address. (pg. 2, lines 20-23).

The present disclosure addresses a routing device with a method for blocking these and other types of attacks by analyzing incoming data packets. (pg. 5, lines 17-19). For example, for address spoofing attacks, incoming packets should not be the same as outgoing packets. (pg. 5, lines 25-26). Therefore, a routing device may intelligently analyze incoming packets, match them against known patterns for attack strategies, and respond appropriately to attempted attacks. (pg. 6, lines 3-6).

According to one embodiment, a method for blocking an attack on a private network implemented by a routing device interconnecting the private network to a public network is disclosed. (pg. 5, lines 17-19). The method comprises receiving a request for connection from an initiator, over the public network. (pg. 7, lines 14-15). An acknowledgment is requested from the initiator of the request and it is determined whether the acknowledgment has been received within a predetermined amount of time. (pg. 7, lines 15-18). If the acknowledgment is not received within the predetermined amount of time, the request is denied. (pg. 7, lines 18-21).

According to a further embodiment, a method for blocking an attack on a private network implemented by a routing device interconnecting the private network to a public network is disclosed. (pg. 5, lines 17-19). The method comprises receiving an incoming data

[1] All citations in this section of the Appeal Brief are to Appellants' originally filed specification.

packet from the public network. (pg. 6, line 25). A source address of the data packet is compared against known internal addresses of the private network and it is determined if the source address matches a known internal address. (pg. 6, lines 25-28). If there is a match, the data packet is dropped, a header of the data packet is analyzed, and information regarding a history of the packet is determined. (pg. 6, line 29-pg. 7, line 4). Additionally, if there is a match, a real source of the data packet is determined using the information regarding the history of the packet and additional data packets received from the real source of the data packet are refused to be processed. (pg. 7, lines 2-9).

With regard to the independent claims currently under Appeal, Appellants provide the following concise explanation of the subject matter recited in the claim elements. For brevity, Appellants do not necessarily identify every portion of the Specification and drawings relevant to the recited claim elements. Additionally, this explanation should not be used to limit Appellants' claims but is intended to assist the Board in considering the Appeal of this Application.

For example, Claim 1 recites the following:

> A method for blocking an attack on a private network implemented by a routing device interconnecting the private network to a public network, comprising: (e.g., pg. 5, lines 17-19; Figure 1)
> receiving a request for connection from an initiator, over the public network; (e.g., pg. 7, lines 14-15)
> requesting an acknowledgment from the initiator of the request; (e.g., pg. 7, lines 15-16)
> determining whether the acknowledgment has been received within a predetermined amount of time; (e.g., pg. 7, lines 17-18) and
> denying the request if the acknowledgment is not received within the predetermined amount of time. (e.g., pg. 7, lines 18-21)

As another example, Claim 15 recites the following:

> A method for blocking an attack on a private network implemented by a routing device interconnecting the private network to a public network, comprising: (e.g., pg. 5, lines 17-19; Figure 1)
> receiving an incoming data packet from the public network; (e.g., pg. 6, line 25)
> comparing a source address of the data packet against known internal addresses of the private network; (e.g., pg. 6, lines 25-27)
> determining if the source address matches a known internal address; (e.g., pg. 6, lines 27-28) and
> if there is a match: (e.g., pg. 6, line 29-pg. 7, line 1)
> dropping the data packet; (e.g., pg. 7, lines 1-2)

analyzing a header of the data packet; (e.g., pg. 7, lines 2-4)

determining information regarding a history of the packet; (e.g., pg. 7, lines 2-4)

determining a real source of the data packet using the information regarding the history of the packet; (e.g., pg. 7, lines 2-4) and

refusing to process any additional data packets received from the real source of the data packet. (e.g., pg. 7, lines 6-9)

As another example, Claim 27 recites the following:

A method for blocking an attack on a private network implemented by a routing device interconnecting the private network to a public network, comprising: (e.g., pg. 5, lines 17-19; Figure 1)

receiving a request for connection from an initiator, over the public network; (e.g., pg. 7, lines 14-15)

requesting an acknowledgment from the initiator of the request; (e.g., pg. 7, lines 15-16)

determining whether the acknowledgment has been received within a predetermined amount of time; (e.g., pg. 7, lines 17-18)

denying the request if the acknowledgment is not received within the predetermined amount of time; (e.g., pg. 7, lines 18-21)

comparing a source address of the request for connection with known internal addresses of the private network; (e.g., pg. 6, lines 25-27)

determining if the source address matches a known internal address; (e.g., pg. 6, lines 27-28) and

refusing to process the request for connection if there is a match. (e.g., pg. 7, lines 6-9)

As another example, Claim 28 recites the following:

A system for blocking an attack on a private network, comprising: (e.g., pg. 5, lines 17-19; Figure 1)

a routing device being operable to interconnect a private network to a public network, the routing device being further operable to: (e.g., pg. 5, lines 17-19; Figure 1)

receive a request for connection from an initiator, over the public network; (e.g., pg. 7, lines 14-15)

request an acknowledgment from the initiator of the request; (e.g., pg. 7, lines 15-16)

determine whether the acknowledgment has been received within a predetermined amount of time; (e.g., pg. 7, lines 17-18) and

deny the request if the acknowledgment is not received within the predetermined amount of time. (e.g., pg. 7, lines 18-21)

As another example, Claim 29 recites the following:

A system for blocking an attack on a private network, comprising: (e.g., pg. 5, lines 17-19; Figure 1)

a routing device being operable to interconnect the private network and a public network, the routing device being further operable to: (e.g., pg. 5, lines 17-19; Figure 1)

receive an incoming data packet from the public network; (e.g., pg. 6, line 25)

compare a source address of the data packet against known internal addresses of the private network; (e.g., pg. 6, lines 25-27)

determine if the source address matches a known internal address; (e.g., pg. 6, lines 27-28) and

if there is a match: (e.g., pg. 6, line 29-pg. 7, line 1)

drop the data packet; (e.g., pg. 7, lines 1-2)

analyze a header of the data packet; (e.g., pg. 7, lines 2-4)

determine information regarding a history of the packet; (e.g., pg. 7, lines 2-4)

determine a real source of the data packet using the information regarding the history of the packet; (e.g., pg. 7, lines 2-4) and

refuse to process any additional data packets received from the real source of the data packet. (e.g., pg. 7, lines 6-9)

As another example, Claim 30 recites the following:

A system for blocking an attack on a private network, comprising: (e.g., pg. 5, lines 17-19; Figure 1)

means for interconnecting a private network to a public network; (e.g., pg. 5, lines 17-19; Figure 1)

means for receiving a request for connection from an initiator, over the public network; (e.g., pg. 7, lines 14-15)

means for requesting an acknowledgment from the initiator of the request; (e.g., pg. 7, lines 15-16)

means for determining whether the acknowledgment has been received within a predetermined amount of time; (e.g., pg. 7, lines 17-18) and

means for denying the request if the acknowledgment is not received within the predetermined amount of time. (e.g., pg. 7, lines 18-21)

As another example, Claim 31 recites the following:

A system for blocking an attack on a private network, comprising: (e.g., pg. 5, lines 17-19; Figure 1)

means for interconnecting the private network and a public network; (e.g., pg. 5, lines 17-19; Figure 1)

means for receiving an incoming data packet from the public network; (e.g., pg. 6, line 25)

means for comparing a source address of the data packet against known internal addresses of the private network; (e.g., pg. 6, lines 25-27)

means for determining if the source address matches a known internal address; (e.g., pg. 6, lines 27-28) and

if there is a match, means for: (e.g., pg. 6, line 29-pg. 7, line 1)

dropping the data packet; (e.g., pg. 7, lines 1-2)

analyzing a header of the data packet; (e.g., pg. 7, lines 2-4)

determining information regarding a history of the packet; (e.g., pg. 7, lines 2-4)

determining a real source of the data packet using the information regarding the history of the packet; (e.g., pg. 7, lines 2-4) and

refusing to process any additional data packets received from the real source of the data packet. (e.g., pg. 7, lines 6-9)

As another example, Claim 32 recites the following:

Software embodied in a computer-readable medium, the computer-readable medium comprising code operable to: (e.g., pg. 7, lines 31-32)

interconnect a private network to a public network; (e.g., pg. 5, lines 17-19; Figure 1)

receive a request for connection from an initiator, over the public network; (e.g., pg. 7, lines 14-15)

request an acknowledgment from the initiator of the request; (e.g., pg. 7, lines 15-16)

determine whether the acknowledgment has been received within a predetermined amount of time; (e.g., pg. 7, lines 17-18) and

deny the request if the acknowledgment is not received within the predetermined amount of time. (e.g., pg. 7, lines 18-21)

As another example, Claim 33 recites the following:

Software embodied in a computer-readable medium, the computer-readable medium comprising code operable to: (e.g., pg. 7, lines 31-32)

receive an incoming data packet from the public network; (e.g., pg. 6, line 25)

compare a source address of the data packet against known internal addresses of the private network; (e.g., pg. 6, lines 25-27)

determine if the source address matches a known internal address; (e.g., pg. 6, lines 27-28) and

if there is a match: (e.g., pg. 6, line 29-pg. 7, line 1)

drop the data packet; (e.g., pg. 7, lines 1-2)

analyze a header of the data packet; (e.g., pg. 7, lines 2-4)

determine information regarding a history of the packet; (e.g., pg. 7, lines 2-4)

determine a real source of the data packet using the information regarding the history of the packet; (e.g., pg. 7, lines 2-4) and

refuse to process any additional data packets received from the real source of the data packet. (e.g., pg. 7, lines 6-9)

Grounds of Rejection to be Reviewed on Appeal

Appellants request the Board to review:

I. the Examiner's rejection of Claims 1-10, 15-21, and 27-33 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,061,650 to Malkin et al. ("*Malkin*"); and

II. the Examiner's rejection of Claims 11-14, and 22-26 under 35 U.S.C. § 103(a) as being unpatentable over *Malkin* in view of U.S. Application No. 2003/0053170 to Levinson et al. ("*Levinson*").

Argument

Appellants have made an effort to group claims to reduce the burden on the Board, as contemplated by 37 C.F.R. § 41.37(c)(l)(vii). Where appropriate, Appellants present arguments as to why particular claims subject to a ground of rejection are separately patentable from other claims subject to the same ground of rejection. To reduce the number of groups and thereby reduce the burden on the Board, Appellants do not argue individually every claim that recites patentable distinctions over the references cited by the Examiner, particularly in light of the clear allowability of Appellants' independent claims. The claims of each group provided below may be deemed to stand or fall together for purposes of this Appeal.

Appellants have concluded that the claims may be grouped together as follows:

1. Group 1 may include Claims 1-14, 27-28, 30, and 32; and
2. Group 2 may include Claims 15-26, 29, 31, and 33.

I. Claims 1-10, 15-21, and 27-33 are allowable over *Malkin*.

Group 1: Claims 1-10, 27-28, 30, and 32 are allowable over *Malkin*.

Claim 1 teaches a method comprising receiving a request for connection from an initiator, over a public network and requesting an acknowledgment from the initiator of the request. Claim 1 further teaches determining whether the acknowledgment has been received within a predetermined amount of time and denying the request if the acknowledgment is not received within the predetermined amount of time. Appellants respectfully contend that *Malkin* fails to disclose each and every one of these limitations.

Malkin teaches a method for "transparently providing mobile functionality to a remote node." *Malkin*, col. 1, lines 64-65. This includes a user dialing into a Remote Access Server (RAS) through a remote node. *Malkin*, col. 2, lines 26-27. The RAS then generates and sends a remote authentication request to an authentication server. *Malkin*, col. 2, lines 42-44. Once the user is authenticated by the authentication server, the RAS generates and sends a tunnel registration request to an appropriate gateway. *Malkin*, col. 2, lines 58-61.

The Examiner's initial rejection of Claim 1 appears to be based in part on a misinterpretation of Claim 1. In the Final Office Action, the Examiner appears to read the limitation "requesting an acknowledgment from the initiator of the request" as requiring a

request for acknowledgment "coming 'from the initiator of the request.'" *See Final Office Action*, pg. 2, paragraph 2.2 (emphasis added). Appellants respectfully point out that Claim 1 does not require a request for acknowledgment coming from the initiator; rather it discloses "requesting an acknowledgment from the initiator." Under this proper reading of Claim 1, Appellants respectfully maintain that the tunnel registration request does not disclose "requesting an acknowledgment from the initiator of the request." This is further supported by the Examiner's own attempted "mapping" of claim elements. In rejecting Claim 1, the Examiner appears to rely on the RAS of *Malkin* as disclosing the "initiator" of Claim 1. *See Final Office Action*, pg. 4. Under the Examiner's mapping, which Appellants do not necessarily agree with, *Malkin* discloses the RAS (i.e. initiator) generating a tunnel registration request and sending it to an appropriate gateway. Therefore, the RAS requests registration from the gateway, and nothing is requested from the RAS (i.e. initiator). Thus, *Malkin* fails to disclose "requesting an acknowledgment from the initiator of the request."

In the Advisory Action, the Examiner maintains the rejection of Claim 1, albeit on different reasoning. Instead of relying on the tunnel registration request, the Examiner now relies on portions of the PPP authentication phase as disclosing "requesting an acknowledgment from the initiator of the request." *Advisory Action*, pg. 2. Specifically, the Examiner relies on portions of *Malkin* that disclose the PPP authentication phase begun by "the RAS sending a Challenge Handshake Authentication Protocol (CHAP) Challenge or Password Authentication Protocol (PAP) message to the remote node." *Malkin*, col. 3, lines 34-39. In response, the remote node passes user authentication information to the RAS, which the RAS then uses to query the TMS for additional information needed to complete authentication of the remote node via a remote AS. *Malkin*, col. 3, lines 40-50. The Examiner states that the "disclosure of the RAS responding to the CHAP or PAP of the node it originally originated the communication with is understand [sic] to read upon the argued claim limitations." *Advisory Action*, pg. 2. Appellants respectfully contend that this still fails to disclose the limitation "requesting an acknowledgment from the initiator of the request."

First of all, it is unclear to Appellants how the RAS "responds" to the CHAP or PAP. *Malkin* makes it clear that the CHAP Challenge or PAP message are things that are sent by the RAS. *Malkin*, col. 3, lines 34-39. Nevertheless, the newly cited portions merely disclose that "the remote node passes a set of user authentication information to the RAS." *Malkin*, col. 3, lines 40-41. Merely sending user authentication information does not disclose

"requesting an acknowledgment from the initiator of the request." For at least these reasons, Appellants respectfully contend that Claim 1 is patentably distinguishable from *Malkin*.

Similar to Claim 1, Claims 27, 28, 30, and 32 include elements generally directed toward receiving a request for connection from an initiator and requesting an acknowledgment from the initiator of the request. Therefore, Appellants respectfully contend that Claims 27, 28, 30, and 32 are patentably distinguishable from *Malkin* for at least the same reasons discussed above with regard to Claim 1.

Claims 2-10 depend, either directly or indirectly, from Claim 1 and incorporate all the limitations thereof. Therefore, Appellants respectfully contend that Claims 2-10 are patentably distinguishable from *Malkin* for at least the same reasons discussed above with regard to Claim 1.

Group 2: Claims 15-21, 29, 31, and 33 are allowable over *Malkin*.

Claim 15 teaches a method comprising receiving an incoming data packet from a public network, comparing a source address of the data packet against known internal addresses of the private network, and determining if the source address matches a known internal address. If there is a match, Claim 15 teaches dropping the data packet, analyzing a header of the data packet, determining information regarding history of the packet, determining a real source of the data packet using the information regarding the history, and refusing to process any additional data packets received from the real source of the data packet.

As described above, *Malkin* teaches a method for "transparently providing mobile functionality to a remote node." *Malkin*, col. 1, lines 64-65. This includes a user dialing into a Remote Access Server (RAS) through a remote node. *Malkin*, col. 2, lines 26-27. The RAS then uses information from the remote node to query a Tunnel Management System (TMS) for additional information needed to complete authentication of the remote node. *Malkin*, col. 3, lines 40-50. This information may include the address of the gateway to the remote node's home network. *Malkin*, col. 2, lines 30-35. Appellants respectfully contend that finding the address of a gateway to the remote node's home network does not disclose "comparing a source address of the data packet against known internal addresses of the private network" and "determining if the source address matches a known internal address."

Furthermore, *Malkin* discloses that if an entry is not found in the TMS database, the connection between the RAS and the remote node will be terminated. *Malkin*, col. 3, lines 57-61. First of all, Appellants respectfully contend that this lack of an entry does not disclose "a match" between a source address and a known internal address. Second, even if this is a match, which Appellants do not concede, *Malkin* only discloses terminating the connection as a result. *Malkin* does not disclose analyzing a header of a data packet, determining information regarding the history of the packet, or determining a real source of the data packet using the history information. Furthermore, Appellants respectfully contend that merely terminating a connection does not disclose "refusing to process any additional data packets received from the real source of the data packet." For at least these reasons, Appellants respectfully request reconsideration and allowance of Claim 15.

Similar to Claim 15, Claims 29, 31, and 33 include elements generally directed toward receiving an incoming data packet, comparing the source address of the data packet against known internal addresses of a private network, and, if there is a match, refusing to process any additional data packets received from the real source of the data packet. Therefore, Appellants respectfully request reconsideration and allowance of Claims 29, 31, and 33 for at least the same reasons discussed above with regard to Claim 15.

Claims 16-21 depend, either directly or indirectly, from Claim 15 and incorporate all the limitations thereof. Therefore, Appellants respectfully request reconsideration and allowance of Claims 16-21 for at least the same reasons discussed above with regard to Claim 15.

II. Claims 11-14 and 22-26 are allowable over the proposed *Malkin-Levinson* combination.

Group 1: Claims 11-14 are allowable over the proposed *Malkin-Levinson* combination.

Claims 11-14 depend indirectly from Claim 1, and incorporate all the limitations thereof. In rejecting Claims 11-14, the Examiner relies on *Malkin* as disclosing each of the limitations of Claim 1. However, as stated above, *Malkin* fails to disclose each of the limitations of Claim 1. *Levinson* fails to cure this deficiency. Therefore, Appellants

respectfully contend that Claims 11-14 are allowable for at least the same reasons as discussed above with regard to Claim 1.

Additionally, *Levinson* merely describes an optoelectronic device that may identify and process data packets that have destination addresses matching the predefined address assigned to the optoelectronic device. *Levinson*, ¶ 0010. However, *Levinson* fails to disclose, teach, or suggest determining additional information about a source of a request for connection, as required by Claims 11-14. Therefore, for at least these reasons, Appellants respectfully request reconsideration and allowance of Claims 11-14.

Group 2: Claims 22-26 are allowable over the proposed *Malkin-Levinson* combination.

Claims 22-26 depend, either directly or indirectly, from Claim 15 and incorporate all the limitations thereof. In rejecting Claims 22-26, the Examiner relies on *Malkin* as disclosing each of the limitations of Claim 15. However, as stated above, *Malkin* fails to disclose each of the limitations of Claim 15. *Levinson* fails to cure this deficiency. Therefore, Appellants respectfully contend that Claims 22-26 are allowable for at least the same reasons as discussed above with regard to Claim 15.

Additionally, *Levinson* merely describes an optoelectronic device that may identify and process data packets that have destination addresses matching the predefined address assigned to the optoelectronic device. *Levinson*, ¶ 0010. However, *Levinson* fails to disclose, teach, or suggest determining additional information about a source of a request for connection, as required by Claims 22-26. Therefore, for at least these reasons, Appellants respectfully request reconsideration and allowance of Claims 22-26.

Conclusion

Appellants have demonstrated that, for at least the foregoing reasons, the present invention, as claimed, is clearly patentable over the references cited by the Examiner. Therefore, Appellants respectfully request the Board to reverse the final rejection of the Examiner and instruct the Examiner to issue a Notice of Allowance of all pending claims.

The Commissioner is hereby authorized to charge the large entity fee of $510.00 under 37 C.F.R. §§1.191(a) and 1.17(b) for filing this Appeal Brief to Deposit Account No. 02-0384 of Baker Botts L.L.P. The Commissioner is authorized to charge any additional fees and/or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Appellant

Luke K. Pedersen
Reg. No. 45,003

Date: 8-20-08

CORRESPONDENCE ADDRESS:
Customer No. **05073**

Appendix A: Claims on Appeal

1. A method for blocking an attack on a private network implemented by a routing device interconnecting the private network to a public network, comprising:

receiving a request for connection from an initiator, over the public network;

requesting an acknowledgment from the initiator of the request;

determining whether the acknowledgment has been received within a predetermined amount of time; and

denying the request if the acknowledgment is not received within the predetermined amount of time.

2. The method of Claim 1, wherein the public network is the Internet.

3. The method of Claim 2, wherein the routing device is a firewall providing access to the Internet.

4. The method of Claim 1, further comprising processing the request if the acknowledgement is received.

5. The method of Claim 1, further comprising adding an IP address of the initiator to a cache of IP addresses if the acknowledgement is not received.

6. The method of Claim 5, further comprising denying access through the routing device to any IP address on the cache of IP addresses.

7. The method of Claim 1, further comprising storing information about the initiator on a system log for analysis by the system administrator.

8. The method of Claim 1, further comprising storing information about the request for connection on a system log for analysis by the system administrator.

9. The method of Claim 1, further comprising determining if a prior request for an acknowledgement has been sent to an IP address associated with the initiator and been unacknowledged within a predetermined amount of time, if the acknowledgement is not received.

10. The method of Claim 1, further comprising using diagnostic tools to determine additional information about a source of the request for connection.

11. The method of Claim 10, wherein using diagnostic tools to determine additional information about a source of the request for connection comprises using trace root diagnostic tools to determine information about the source of the request for connection.

12. The method of Claim 10, wherein using diagnostic tools to determine additional information about a source of the request for connection comprises using ping diagnostic tools to determine information about the source of the request for connection.

13. The method of Claim 10, wherein using diagnostic tools to determine additional information about a source of the request for connection comprises using NS lookup diagnostic tools to determine information about the source of the request for connection.

14. The method of Claim 10, further comprising forwarding the additional information to a system administrator via electronic mail.

15. A method for blocking an attack on a private network implemented by a routing device interconnecting the private network to a public network, comprising:

receiving an incoming data packet from the public network;

comparing a source address of the data packet against known internal addresses of the private network;

determining if the source address matches a known internal address; and

if there is a match:

dropping the data packet;

analyzing a header of the data packet;

determining information regarding a history of the packet;

determining a real source of the data packet using the information regarding the history of the packet; and

refusing to process any additional data packets received from the real source of the data packet.

16. The method of Claim 15, further comprising storing data about the data packet on a system log, for use and analysis by a system administrator.

17. The method of Claim 15, wherein the public network is the Internet.

18. The method of Claim 17, wherein the routing device is a firewall providing access to the Internet.

19. The method of Claim 15, further comprising forwarding the data packet to the private network if there is not a match.

20. The method of Claim 15, further comprising adding an IP address of the data packet to a cache of IP addresses if there is a match.

21. The method of Claim 20, further comprising denying access through the routing device to any IP address on the cache of IP addresses.

22. The method of Claim 15, further comprising using diagnostic tools to determine additional information about a source of the data packet.

23. The method of Claim 22, wherein using diagnostic tools to determine additional information about a source of the data packet comprises using trace root diagnostic tools to determine additional information about the source of the data packet.

24. The method of Claim 22, wherein using diagnostic tools to determine additional information about a source of the data packet comprises using ping diagnostic tools to determine additional information about the source of the data packet.

25. The method of Claim 22, wherein using diagnostic tools to determine additional information about a source of the data packet comprises using NS lookup diagnostic tools to determine additional information about the source of the data packet.

26. The method of Claim 22, further comprising forwarding the additional information to a system administrator via electronic mail.

27. A method for blocking an attack on a private network implemented by a routing device interconnecting the private network to a public network, comprising:

receiving a request for connection from an initiator, over the public network;

requesting an acknowledgment from the initiator of the request;

determining whether the acknowledgment has been received within a predetermined amount of time;

denying the request if the acknowledgment is not received within the predetermined amount of time;

comparing a source address of the request for connection with known internal addresses of the private network;

determining if the source address matches a known internal address; and

refusing to process the request for connection if there is a match.

28. A system for blocking an attack on a private network, comprising:

a routing device being operable to interconnect a private network to a public network, the routing device being further operable to:

receive a request for connection from an initiator, over the public network;

request an acknowledgment from the initiator of the request;

determine whether the acknowledgment has been received within a predetermined amount of time; and

deny the request if the acknowledgment is not received within the predetermined amount of time.

29. A system for blocking an attack on a private network, comprising:

a routing device being operable to interconnect the private network and a public network, the routing device being further operable to:

receive an incoming data packet from the public network;

compare a source address of the data packet against known internal addresses of the private network;

determine if the source address matches a known internal address; and

if there is a match:

drop the data packet;

analyze a header of the data packet;

determine information regarding a history of the packet;

determine a real source of the data packet using the information regarding the history of the packet; and

refuse to process any additional data packets received from the real source of the data packet.

30. A system for blocking an attack on a private network, comprising:

means for interconnecting a private network to a public network;

means for receiving a request for connection from an initiator, over the public network;

means for requesting an acknowledgment from the initiator of the request;

means for determining whether the acknowledgment has been received within a predetermined amount of time; and

means for denying the request if the acknowledgment is not received within the predetermined amount of time.

31. A system for blocking an attack on a private network, comprising:

means for interconnecting the private network and a public network;

means for receiving an incoming data packet from the public network;

means for comparing a source address of the data packet against known internal addresses of the private network;

means for determining if the source address matches a known internal address; and

if there is a match, means for:

dropping the data packet;

analyzing a header of the data packet;

determining information regarding a history of the packet;

determining a real source of the data packet using the information regarding the history of the packet; and

refusing to process any additional data packets received from the real source of the data packet.

32. Software embodied in a computer-readable medium, the computer-readable medium comprising code operable to:

interconnect a private network to a public network;

receive a request for connection from an initiator, over the public network;

request an acknowledgment from the initiator of the request;

determine whether the acknowledgment has been received within a predetermined amount of time; and

deny the request if the acknowledgment is not received within the predetermined amount of time.

33. Software embodied in a computer-readable medium, the computer-readable medium comprising code operable to:

receive an incoming data packet from the public network;

compare a source address of the data packet against known internal addresses of the private network;

determine if the source address matches a known internal address; and

if there is a match:

drop the data packet;

analyze a header of the data packet;

determine information regarding a history of the packet;

determine a real source of the data packet using the information regarding the history of the packet; and

refuse to process any additional data packets received from the real source of the data packet.

Appendix B: Evidence

(None)

Appendix C: Related Proceedings

The Appellants, the undersigned Attorney for Appellants, and the Assignees know of no applications on appeal that may directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.